IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

UNITED STATES OF AMERICA	)	
	)	
	)	**Case No. 3:19cr130**
	)	
OKELLO T. CHATRIE,	)	
Defendant	)	

RESPONSE TO GOVERNMENT'S NOTICE OF SUPPLEMENTAL AUTHORITY

Okello Chatrie, through counsel, responds as follows to the government's notice of supplemental authority, *see* ECF No. 216, regarding the Fourth Circuit's recent published *en banc* decision in *Leaders of a Beautiful Struggle v. Baltimore Police Department*, --- F.4th ----, 2021 WL 2584408 (4th Cir. June 24, 2021) ("*Leaders*"), which held that accessing a database of high-resolution aerial surveillance photos of large swaths of Baltimore was a search.

To reach this holding, *Leaders* applied the principles of *Carpenter v. United States*, 138 S. Ct. 2206 (2018), beyond the confines of cell site location information ("CSLI"). While, in this case, the government contends that courts have not and should not apply *Carpenter* outside of its specific context, *see* 6/24/21 Tr. at 64, *Leaders* demonstrates that *Carpenter* can and does extend to other types of location data capable of revealing the "privacies of life." *Leaders*, at *8.

In *Leaders*, the data at issue came from a "first-of-its-kind aerial surveillance program" called the Aerial Investigation Research ("AIR") program, operated by the Baltimore Police Department and a private contractor. The program used "planes equipped with high-tech cameras" to surveil 90% of Baltimore for twelve hours each day. *Id.* at *1. An agreement between the police and the contractor "limited the photographic resolution to one pixel per person or vehicle," which were "individually visible, but only as blurred dots or blobs." *Id.* The contractor stored this "AIR data" on its servers for 45 days. When certain crimes occurred, the contractor would prepare

reports for the police containing responsive AIR data from both before and after the crime. *Id.* at *2. Specifically, these reports included the "tracks" of "vehicles and people present at the scene; the locations of those vehicles and people visited; and eventually, the tracks of the people whom those people met with and the locations they came from and went to." *Id.* Such "tracks" are "often shorter snippets of several hours or less." *Id.* at *8.

While there were clear technical differences between AIR data and CSLI, the *Leaders* Court found that *Carpenter* "applies squarely" to this new type of location data. *Id.* at *8. The court recognized that "because the AIR program opens 'an intimate window' into a person's associations and activities," it is akin to the CSLI in *Carpenter* and the GPS data in *United States v. Jones*, 565 U.S. 400 (2012).

It did not matter that the reports provided to police were just "snippets of several hours or less," *id.* at *8, because that information could only be derived by "accessing" (*i.e.*, searching) the full 45-day repository of AIR data. *Id.* at 10. *Leaders* made careful note of the fact that police "access" to any slice, or "track," of location data necessarily entailed the "recording of *all* public movements across Baltimore." *Id.* at *4. "Only after recording movements across Baltimore for twelve hours per day could BPD zero in on specific dates and locations related to its investigations," the court explained. *Id.* at *5. Consequently, *Leaders* considered the denominator—the total number days available to search—not the length of any "track," to conclude that the data constitutes "a 'detailed, encyclopedic,' record of where everyone came and went." *Id.* at *8. In this sense, the AIR data was not truly "short term," because it can only be derived from a search of the "whole of individuals' movements" over 45 days. *Id.* at 11.

The government misconstrues *Leaders* on this point, suggesting that the two hours of Location History data at issue in this case is more consistent with "ordinary police capabilities"

such as "security cameras, being tailed, and being staked out for a time." ECF No. 216 at 2. But as Mr. Chatrie has argued, and as *Leaders* made clear: the "retrospective quality of the data" makes a big difference. *Leaders*, at *8. While "[p]eople understand that they may be filmed by security cameras on city streets, or a police officer could stake out their house and tail them for a time, …capturing everyone's movements outside during the daytime for 45 days goes beyond that ordinary capacity." *Id.* at 11. It "enables police to 'retrace a person's whereabouts,' granting access to otherwise 'unknowable' information." *Id.* at *8. Unlike a stakeout or tail, which would require knowing ahead of time who to follow, the AIR program allowed police to "travel back in time" and observe a target's movements, meaning that "'[w]hoever the suspect turns out to be,' they have 'effectively been tailed' for the prior six weeks." *Id*. This kind of search "transcends mere augmentation of ordinary police capabilities" and is not truly "short-term" like stakeout or tail. For this reason, *Leaders* equates "short term" tracking with "what law enforcement could do '[p]rior to the digital age,'" while describing "prolonged tracking" as that which "can reveal intimate details through habits and patterns." *Id*.

Mr. Chatrie maintains that geofence searches operate in a similar fashion, akin to a time machine for police that has no analog prior to the digital age. *See* ECF No. 29 at 13-14; ECF No. 104 at 14-15. In Mr. Chatrie's case, however, the geofence search entailed "accessing" an even greater trove of precise location data than in *Leaders*. At the time the geofence warrant was executed, Location History data was retained indefinitely on Google's servers,[1] *see* ECF 213 at 4, and it was available for "numerous tens of millions" of people, many multiples the population of Baltimore. *See* ECF No. 205 at 16. Without the ability to search this enormous cache of accounts,

[1] Mr. Chatrie's Location History records date back to when Location History was enabled on his device: July 9, 2018. The search warrant was issued on June 14, 2019. Thus, Mr. Chatrie had 341 days of Location History data available to be searched. Other users may have had Location History enabled since Google began the service in 2009.

then, as in *Leaders*, the government would not have been able to identify devices present at a given place and time. As *Leaders* put it, "the government can deduce such information only because it recorded *everyone's* movements." *Leaders*, at *8.

Leaders also does not support the government's position that "Google's internal filtering processes lack Fourth Amendment significance." ECF No. 216 at 3. Quite the opposite. *Leaders* affirmed that the contractor was a state actor, making its actions attributable to the Baltimore Police Department. *Leaders* at *4 n5. The rationale in *Leaders* was the existence of a contract, *id.*, whereas the rationale in this case is the compulsory nature of the geofence warrant served on Google. *See* ECF No. 205 at 34-35; ECF No. 213 at 1; *see also Skinner v. Railway Labor Executives' Association*, 489 U.S. 602, 614 (1989) (observing that private parties conducting a search under the "compulsion of sovereign authority" are government agents for purposes of the Fourth Amendment). And in *Leaders*, it was the initial search performed by the contractor—across 45 days of data on hundreds of thousands of people—that set this new technology apart from security cameras or physical surveillance. Likewise, Mr. Chatrie maintains that the nature of the initial search, performed by Google at the government's direction, across years of location data belonging to tens of millions of people, is of paramount constitutional significance. As in *Carpenter*, however, the government's position here "fails to contend with the seismic shifts in digital technology that made possible the tracking of not only [Mr. Chatrie's] location, but also everyone else's, not for a short period but for years and years." 138 S. Ct. at 2219.

Finally, it is also significant that *Leaders* found a Fourth Amendment search had occurred even though the AIR data had coverage gaps and the people and cars were intentionally pixilated to obscure their identities. *Leaders*, at *1, *9. As the court found (and as Mr. Chatrie has demonstrated in this case, *see* ECF No. 205 at 22; ECF No. 104 at 27), "identity is easy to deduce

from just a few random points of an individual's movements," a conclusion corroborated by "common sense and ample authority over the last decade." *Leaders*, at *10. This is especially true when the data is coupled with other sources of information, such as surveillance cameras and license plate readers, but the court was clear that a "search" took place any time the government "accessed" the data. *Id.* at *10. In Mr. Chatrie's case, the facts are even stronger. There are no such gaps in Location History data, which is collected every two to six minutes, regardless of whether the phone is in use. *See* ECF No. 205 at 26. And unlike the AIR data in *Leaders*, Location History identifies people not just in public, but also inside of constitutionally protected spaces. Although the *Leaders* court did not have to confront this issue, the court recognized longstanding Supreme Court precedent for the rule that a search occurs when the government uses "technological enhancement of ordinary perception" to obtain information about the interior of a home "that could not otherwise have been obtained" by "naked-eye surveillance." *Id.* at *7 (quoting *Kyllo v. United States*, 533 U.S. 27, 33-35 (2001)); *see also* ECF No. 205 at 32; ECF No. 29 at 14–16; ECF No. 48 at 8–10; ECF No. 109 at 20–21.

Respectfully submitted,
OKELLO T. CHATRIE

By: /s/

Michael W. Price
NY Bar No. 4771697 (*pro hac vice*)
Counsel for Defendant
National Association of Criminal Defense Lawyers
Fourth Amendment Center
1660 L St. NW, 12th Floor
Washington, D.C. 20036
Ph. (202) 465-7615
Fax (202) 872-8690
mprice@nacdl.org

/s/

Laura Koenig

Va. Bar No. 86840
Counsel for Defendant
Office of the Federal Public Defender
701 E Broad Street, Suite 3600
Richmond, VA 23219-1884
Ph. (804) 565-0881
Fax (804) 648-5033
laura_koenig@fd.org

/s/
Paul G. Gill
Va. Bar No. 31461
Counsel for Defendant
Office of the Federal Public Defender
701 E Broad Street, Suite 3600
Richmond, VA 23219-1884
Ph. (804) 565-0870
Fax (804) 648-5033
Paul_gill@fd.org